Proactive Response Strategy for Energy Delivery Systems

Ahmed Fawaz, Carmen Cheh, Uttam Thakore, Atul Bohara, Ben Ujcich, Mohammad Noureddine, Brett Feddersen, and William H. Sanders

GOALS

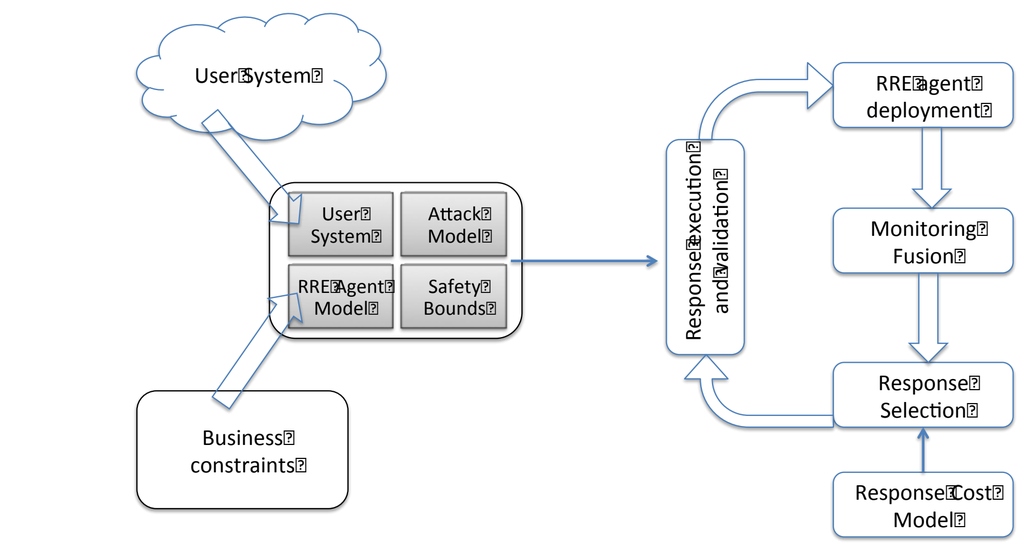
- Reactive response against adversarial attacks, where the response uses knowledge about the power grid's current security state and its security requirements.
- Build RRE as a distributed agent-based system that actively monitors the systems and devises responses.
- Develop new monitors to detect behavioral abnormalities using physical ground truth.
- Define a language for response action deployment.
- Define system-specific tolerance metrics for response decision algorithms.

FUNDAMENTAL QUESTIONS/CHALLENGES

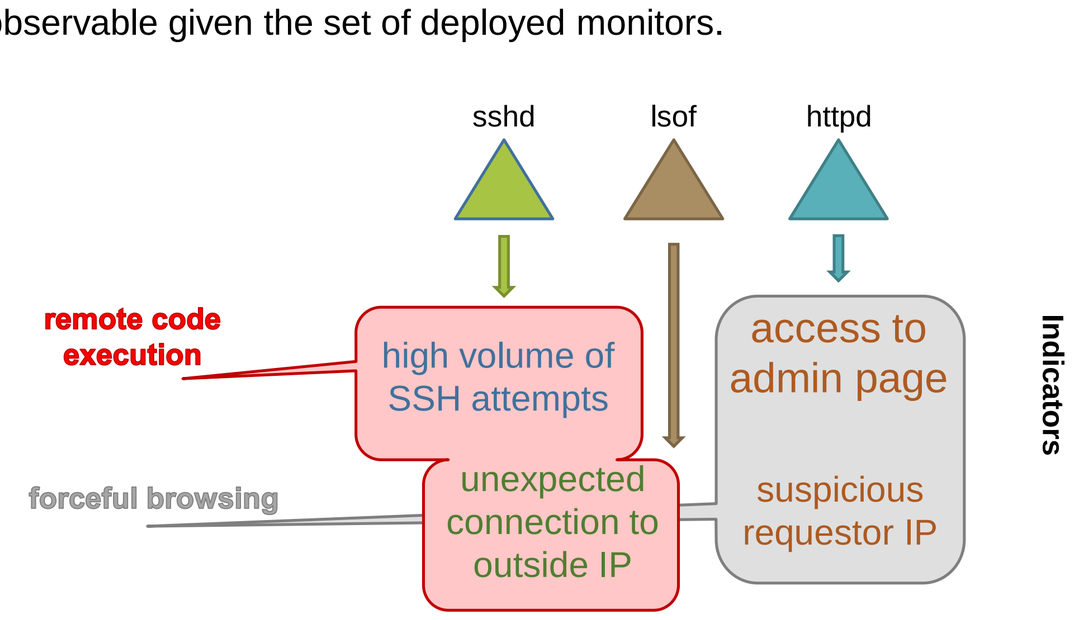
- How do we maintain the state of the system across distributed agents?
- How do we ensure the integrity of the agents if they are part of a compromised host?
- How does using diverse sources of information increase the confidence in monitoring information?
- Can low-level physical information provide a base of trust for monitoring information?
- What is the best metric for tolerance and system performance?
- What is the set of decision algorithms needed to find optimal responses?

RESEARCH PLAN

- Component-level plan for the distributed response engine.



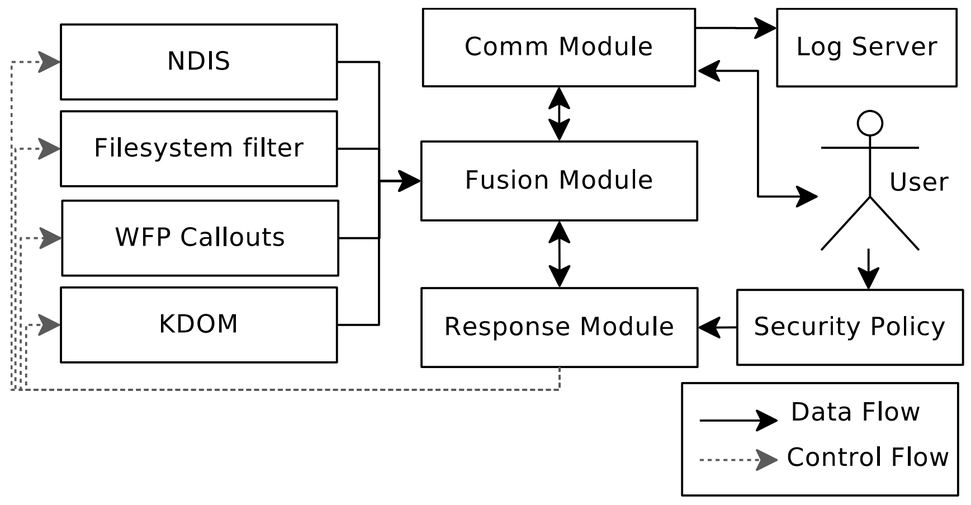
- Optimal offline monitor deployment using information about events to be detected and indicators provided by the monitors.
- **Indicators**: primitives representing semantic information provided by monitors about events in the system.
  - Generated using data from monitors.
- **Events**: occurrences in the system that are symptomatic of an attack or intrusion or are attacks themselves.
  - Events are detectable using sets of indicators (similar to an IDS signature).
- **Detectability**: an event is *detectable* if at least one of its indicator sets is observable given the set of deployed monitors.



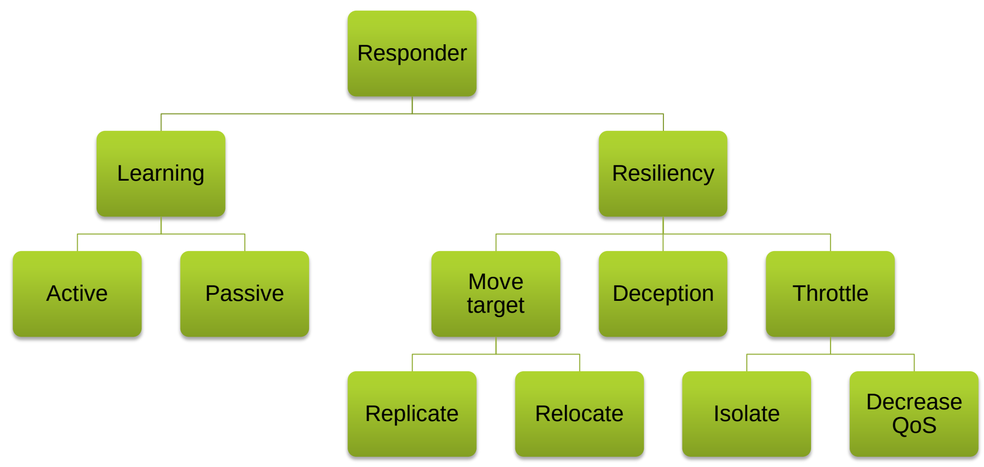
$$\max \; Coverage(\Phi, M_d) + \sum_{\phi=\Phi} (Redundamcy(\phi, M_d) + Confidence(\phi, M_d))$$

RESEARCH PLAN

- Kobra is a kernel-level monitoring engine that collects low-level information for anomaly detection. It generates behavioral baselines of process events for anomaly detection.
- Kobra collects information about the same event from different sources in the kernel for integrity checking.
- A security policy is specified as a predicate on the state of the system.
- A communication module communicates with the user for learning responses and for logging purposes.



- The taxonomy of response actions highlights our response strategy in alternating between learning about an intrusion and containing the attack.
- Learning responses improves the quality of the inferred state of the system by active probing or increasing passive monitoring and fusion.
- Resiliency actions change the system by blocking the attacker, increasing service, and employing deception.



BROADER IMPACT

- The ultimate goal of providing an automated response capability to power grid control rooms will enable quick reaction against security attacks and failures, thus preventing them from causing potentially catastrophic failures.
- The research also advances the study of anomaly detection algorithms and examines the effect of information fusion on accuracy and specificity.

FUTURE EFFORTS

- Design physical models to augment monitor data for integrity checking.
- Design and evaluate response selection algorithms.
- Design and evaluate data fusion algorithms.
- Implement RRE for embedded devices similar to those found in energy delivery systems.
- Develop behavioral anomaly detection algorithms to detect insider attacks.

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY